

THAT WHICH IS CLAIMED IS:

1. A method of providing Internet Protocol
5 Security (IPSec) to a plurality of target hosts in a
cluster of data processing systems which communicate with
a network through a routing communication protocol stack
utilizing a dynamically routable Virtual Internet
Protocol Address (DVIPA) for communications from the
10 plurality of target hosts, the method comprising:

negotiating security associations (SAs) associated
with the DVIPA utilizing an Internet Key Exchange (IKE)
component associated with the routing communication
protocol stack;

15 distributing information about the negotiated SAs to
the target hosts to allow the target hosts to perform
IPSec processing of communications to the network
utilizing the negotiated SAs; and

IPSec processing the communications to the network
20 utilizing the distributed SA information at communication
protocol stacks at respective ones of the plurality of
target hosts.

2. A method according to Claim 1, further
25 comprising the step of storing the distributed
information in a shadow SA caches at the target hosts.

3. A method according to Claim 2, wherein the step
of IPSec processing outbound communications comprises the
30 steps of:

locating an SA stored in the shadow SA cache which

is associated with the outbound communication; and

IPsec processing the outbound communication
utilizing the located SA.

5 4. A method according to Claim 3, further
comprising sending the processed outbound communication
to the network without routing the outbound communication
through the routing communication protocol stack.

10 5. A method according to Claim 3, further
comprising the step of obtaining an IPsec sequence number
associated with the located SA; and

 wherein the step of IPsec processing the outbound
communication utilizing the located SA further comprises
15 the step of IPsec processing the outbound communication
utilizing the located SA and the obtained IPsec sequence
number.

20 6. A method according to Claim 5, wherein the step
of obtaining an IPsec sequence number comprises obtaining
an IPsec sequence number from a coupling facility.

25 7. A method according to Claim 5, wherein the step
of obtaining an IPsec sequence number comprises the step
of obtaining IPsec sequence numbers for a plurality of
outbound communications from a communication protocol
stack at a respective one of the target hosts.

30 8. A method according to Claim 3, further
comprising the step of providing an outbound lifetime
count to the routing communication protocol stack.

9. A method according to Claim 8, wherein the IKE associated with the routing communication protocol stack refreshes the SAs associated with the DVIPA based on the outbound lifesize count.

5

10. A method according to Claim 8, wherein the step of providing an outbound lifesize count comprises the step of sending a cross coupling facility (XCF) message identifying the outbound lifesize count to the routing communication protocol stack.

10

11. A method according to Claim 10, wherein the step of sending an XCF message identifying the outbound lifesize count comprises the step of periodically sending a XCF message identifying the outbound lifesize count for a plurality of IPSec processed communications for a routing communication protocol stack for a respective one of the target hosts.

15

20

12. A method according to Claim 11, wherein the plurality of IPSec processed communications comprises a percentage of a total lifesize count associated with an SA.

25

13. A method according to Claim 12, further comprising the step of dynamically establishing the percentage of the total lifesize count based on whether the IKE has previously refreshed the SA prior to expiration of a lifesize count threshold associated with the SA.

30

14. A system for providing Internet Protocol Security (IPSec) to a plurality of target hosts in a cluster of data processing systems which communicate with a network through a routing communication protocol stack utilizing a dynamically routable Virtual Internet Protocol Address (DVIPA) for communications from the plurality of target hosts, comprising:

means for negotiating security associations (SAs) associated with the DVIPA utilizing an Internet Key Exchange (IKE) component associated with the routing communication protocol stack;

means for distributing information about the negotiated SAs to the target hosts to allow the target hosts to perform IPSec processing of communications to the network utilizing the negotiated SAs; and

means for IPSec processing the communications to the network utilizing the distributed SA information at communication protocol stacks at respective ones of the plurality of target hosts.

15. A system according to Claim 14, further comprising means for storing the distributed information in a shadow SA caches at the target hosts.

16. A system according to Claim 15, wherein the means for IPSec processing outbound communications comprises:

means for locating an SA stored in the shadow SA cache which is associated with the outbound communication; and

means for IPsec processing the outbound

communication utilizing the located SA.

17. A system according to Claim 16, further comprising means for obtaining an IPSec sequence number associated with the located SA; and

wherein the means for IPsec processing the outbound communication utilizing the located SA further comprises means for IPsec processing the outbound communication utilizing the located SA and the obtained IPSec sequence number.

18. A method according to Claim 17, wherein the means for obtaining an IPSec sequence number comprises means for obtaining an IPSec sequence number from a coupling facility.

19. A system according to Claim 17, wherein the means for obtaining an IPSec sequence number comprises means for obtaining IPSec sequence numbers for a plurality of outbound communications from a communication protocol stack at a respective one of the target hosts.

20. A system according to Claim 16, further comprising means for providing an outbound lifesize count to the routing communication protocol stack.

21. A system according to Claim 20, wherein the means for providing an outbound lifesize count comprises means for periodically sending a cross coupling facility (XCF) message identifying the outbound lifesize count for a plurality of IPSec processed communications for a

routing communication protocol stack for a respective one of the target hosts.

22. A system according to Claim 21, wherein the plurality of IPSec processed communications comprises a percentage of a total lifetime count associated with an SA.

23. A system according to Claim 22, further comprising means for dynamically establishing the percentage of the total lifetime count based on whether the IKE has previously refreshed the SA prior to expiration of a lifetime count threshold associated with the SA.

24. A computer program product for providing Internet Protocol Security (IPSec) to a plurality of target hosts in a cluster of data processing systems which communicate with a network through a routing communication protocol stack utilizing a dynamically routable Virtual Internet Protocol Address (DVIPA) for communications from the plurality of target hosts, comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer program code which negotiates security associations (SAs) associated with the DVIPA utilizing an Internet Key Exchange (IKE) component associated with the routing communication protocol stack;

computer program code which distributes

information about the negotiated SAs to the target hosts to allow the target hosts to perform IPSec processing of communications to the network utilizing the negotiated SAs; and

5 computer program code which IPSec processes the communications to the network utilizing the distributed SA information at communication protocol stacks at respective ones of the plurality of target hosts.

10 25. A computer program product according to Claim 24, further comprising computer program code which stores the distributed information in a shadow SA caches at the target hosts.

15 26. A computer program product according to Claim 25, wherein the computer program code which IPSec processes outbound communications comprises:

20 computer program code which locates an SA stored in the shadow SA cache which is associated with the outbound communication; and

computer program code which IPSec processes the outbound communication utilizing the located SA.

25 27. A computer program product according to Claim 26, further comprising computer program code which obtains an IPSec sequence number associated with the located SA; and

30 wherein the computer program code which IPsec processes the outbound communication utilizing the located SA further comprises computer program code which IPsec processes the outbound communication utilizing the

located SA and the obtained IPSec sequence number.

28. A computer program product according to Claim
27, wherein the computer program code which obtains an
5 IPSec sequence number comprises computer program code
which obtains an IPSec sequence number from a coupling
facility.

29. A computer program product according to Claim
10 27, wherein the computer program code which obtains an
IPSec sequence number comprises computer program code
which obtains IPSec sequence numbers for a plurality of
outbound communications from a communication protocol
stack at a respective one of the target hosts.

30. A computer program product according to Claim
15 26, further comprising computer program code which
provides an outbound lifesize count to the routing
communication protocol stack.

31. A computer program product according to Claim
20 30, wherein the computer program code which provides an
outbound lifesize count comprises computer program code
which periodically sends a cross coupling facility (XCF)
25 message identifying the outbound lifesize count for a
plurality of IPSec processed communications for a routing
communication protocol stack for a respective one of the
target hosts.

32. A computer program product according to Claim
30 31, wherein the plurality of IPSec processed

communications comprises a percentage of a total lifesize
count associated with an SA.

33. A computer program product according to Claim
32, further comprising computer program code which
dynamically establishes the percentage of the total
lifesize count based on whether the IKE has previously
refreshed the SA prior to expiration of a lifesize count
threshold associated with the SA.

10